

FIG. 1

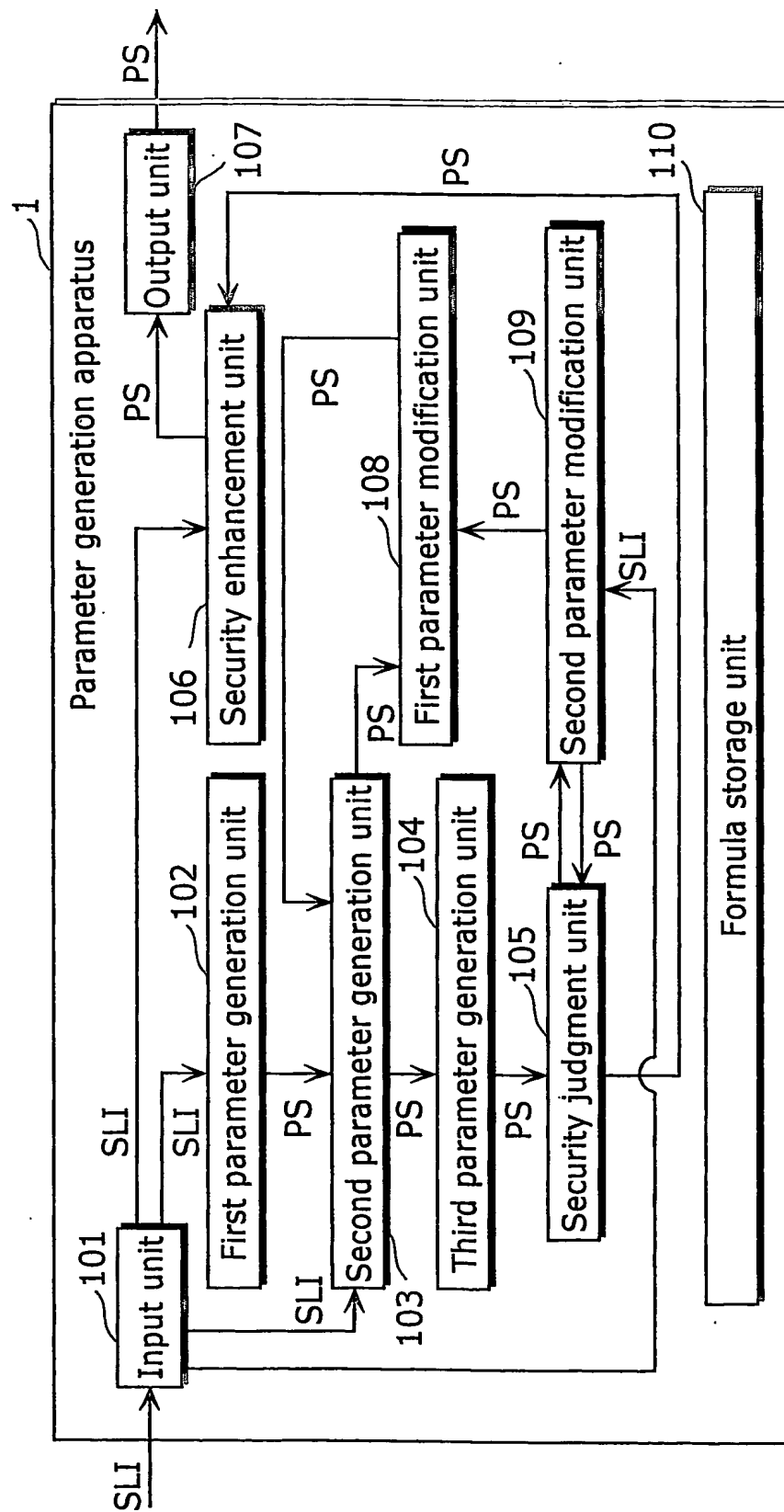


FIG. 2

Parameter N	Decryption time T (seconds)
70	16.587
72	18.68
74	26.497
76	25.869
78	31.182
80	37.76
82	56.442
84	56.359
86	68.174
88	86.6
90	111.78

FIG. 3

110

Formula storage unit	
Lattice constant GL	2.12
Decryption time evaluation formula EF	$\log(T)=0.04N-6.2$
Conditional expression ED	$6d+2df-1<q/2$
Initial security determination formula IF	
$\log(T)=0.2002N-18.884$	

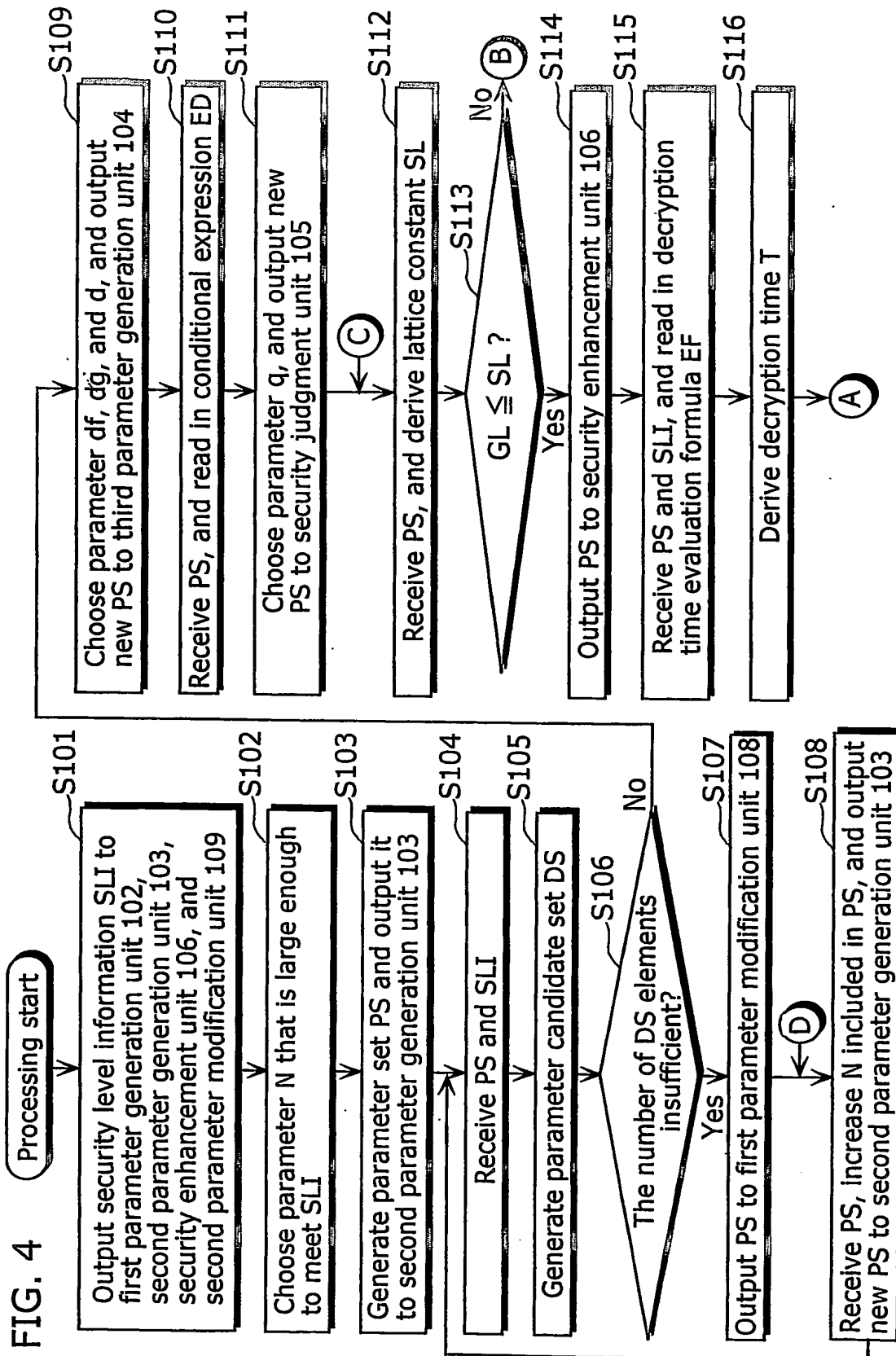


FIG. 5

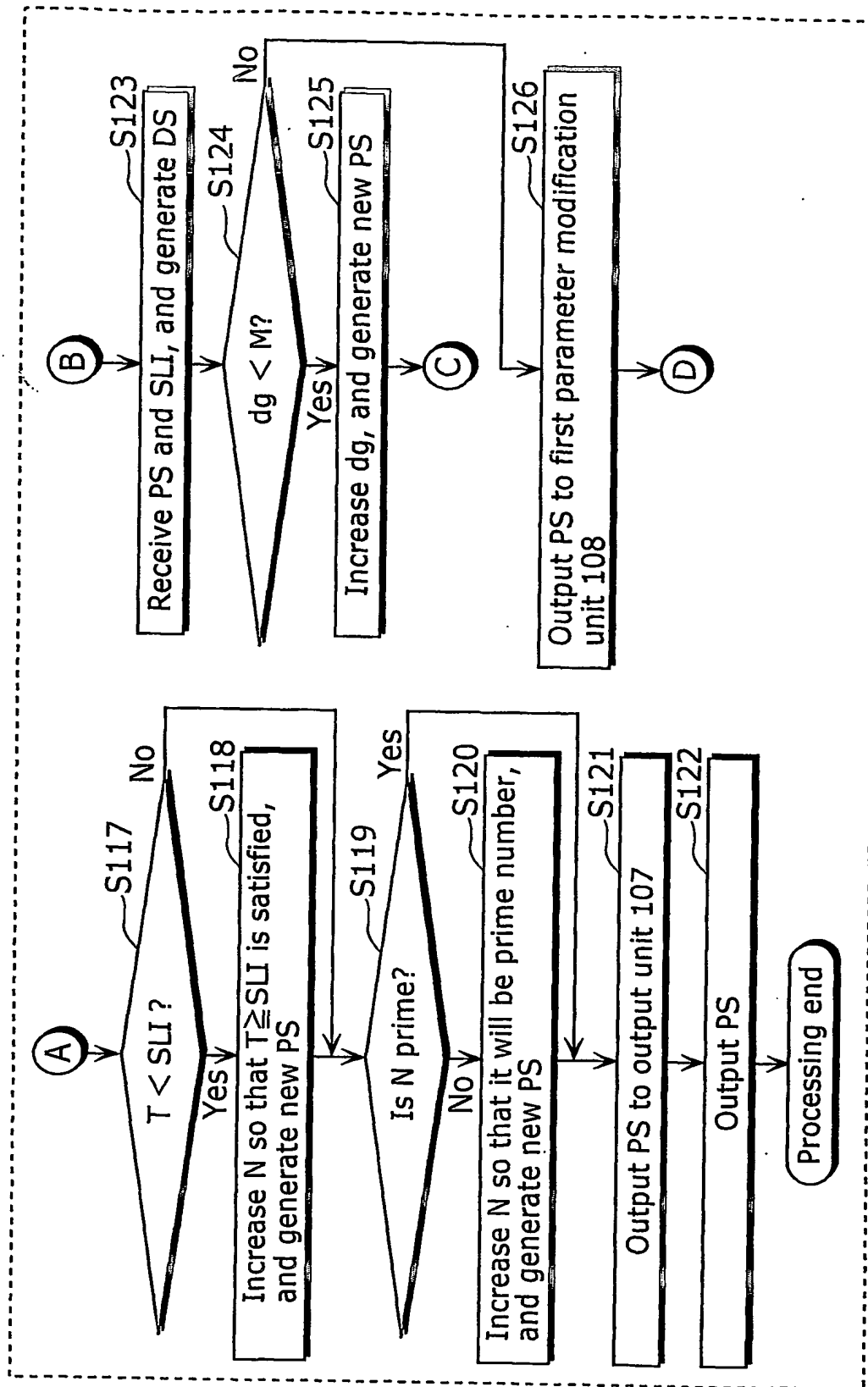


FIG. 6

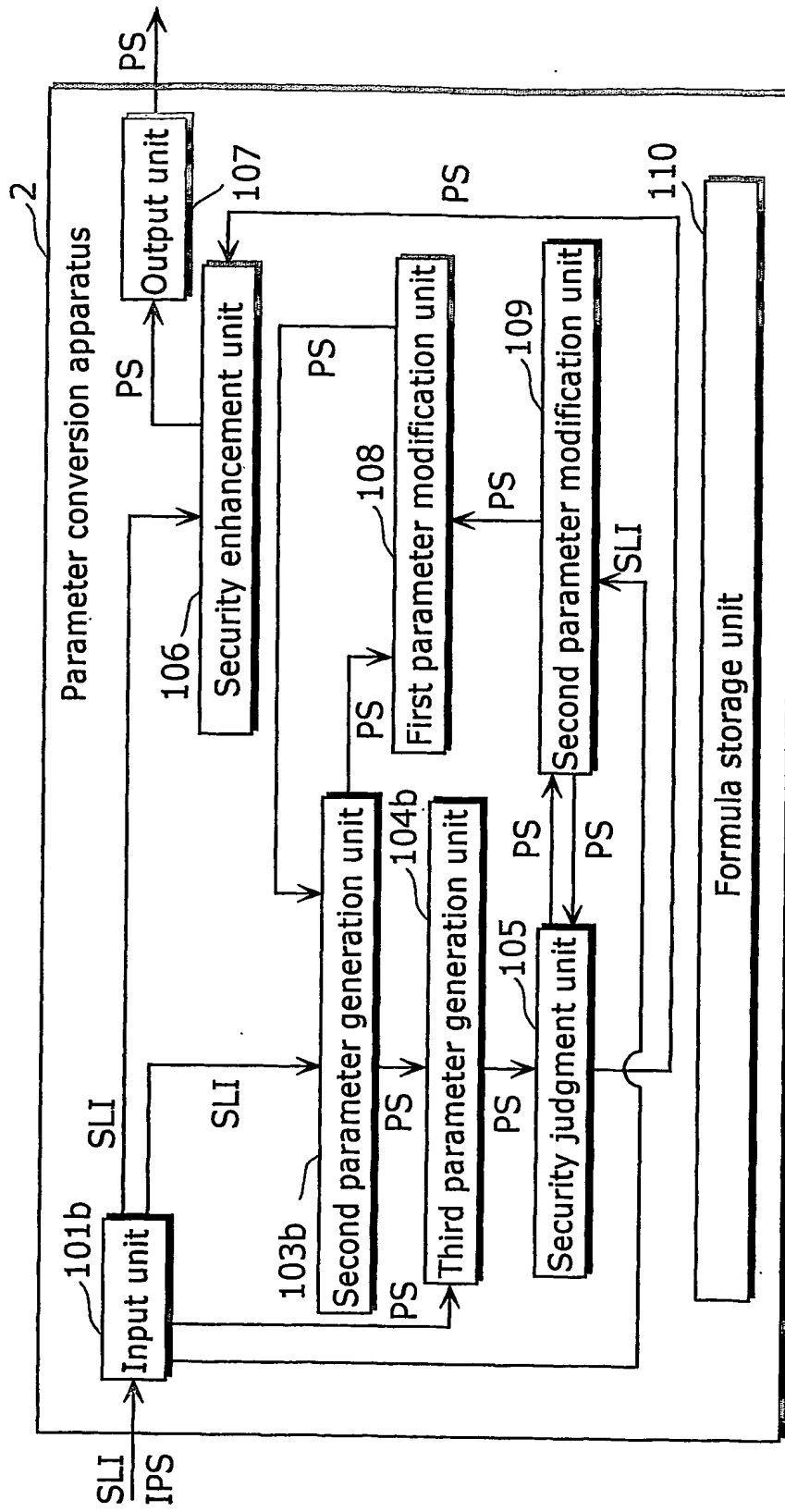


FIG. 7

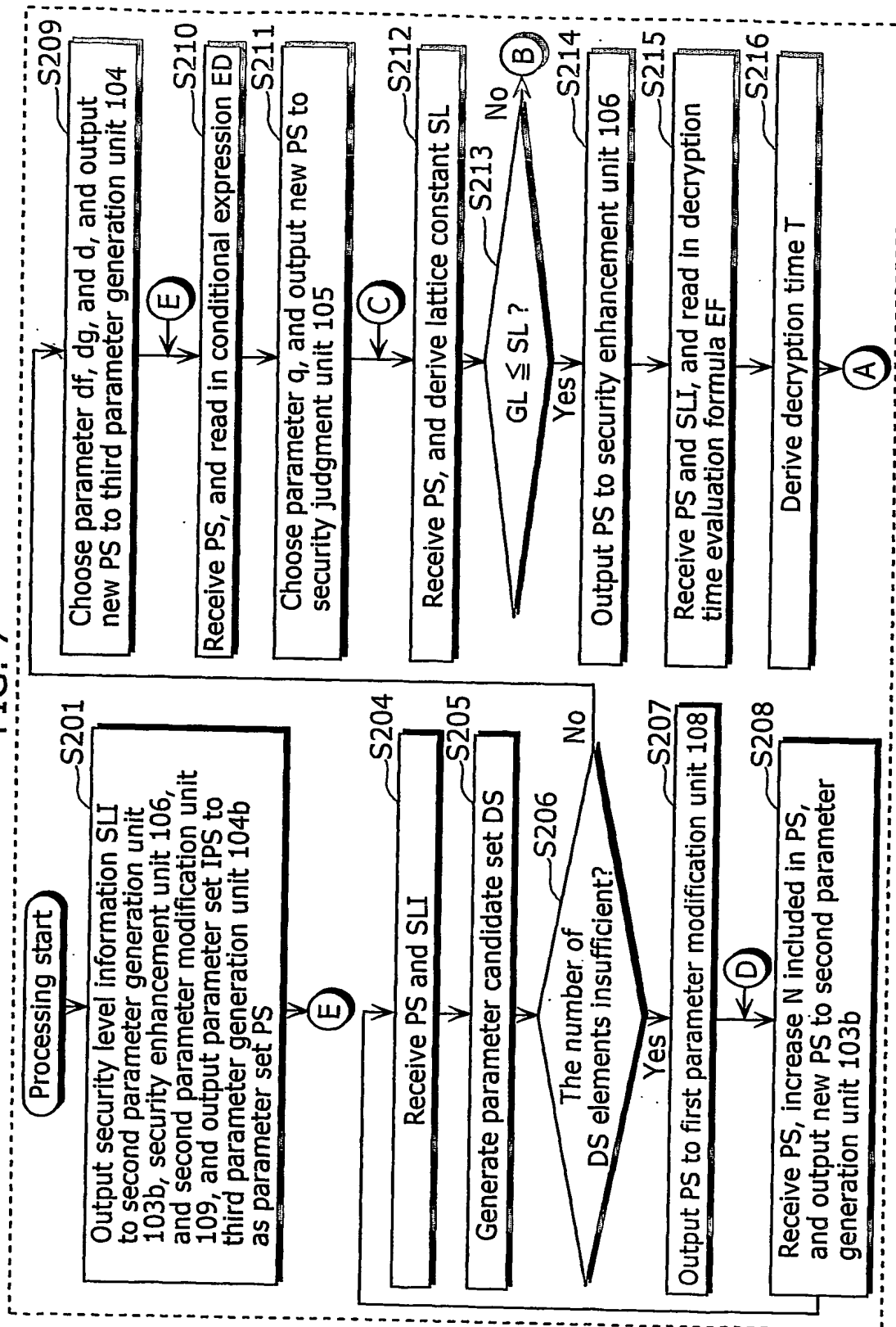


FIG. 8

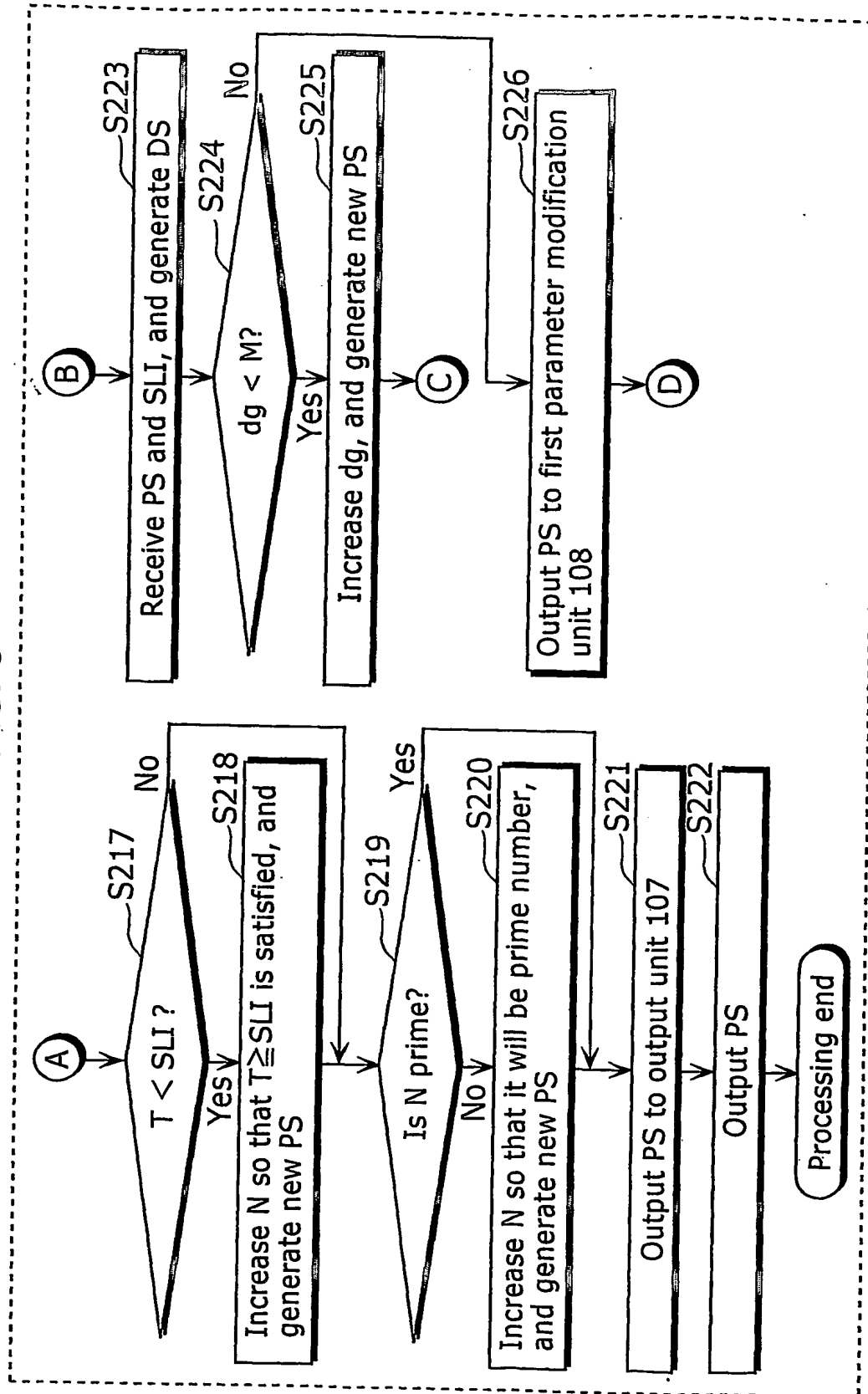


FIG. 9

Security level information SLI	Parameter set IPS
For 512-bit RSA encryption	IPS=(167, 3, 128, 61, 280, 18)
For 1024-bit RSA encryption	IPS=(263, 3, 128, 50, 24, 16)
For 2048-bit RSA encryption	IPS=(503, 3, 256, 217, 72, 55)
:	:

FIG. 10

110

Formula storage unit	
Lattice constant GL	2.12
Decryption time evaluation formula EF	$\log(T) = 0.04N - 6.2$
Lattice constant GL	3.5
Decryption time evaluation formula EF	$\log(T) = 0.08N - 4.8$
Lattice constant GL	4.6
Decryption time evaluation formula EF	$\log(T) = 0.13N - 4.4$
Conditional expression ED	$6d + 2df - 1 < q/2$
Initial security determination formula IF	$\log(T) = 0.2002N - 18.884$

FIG. 11

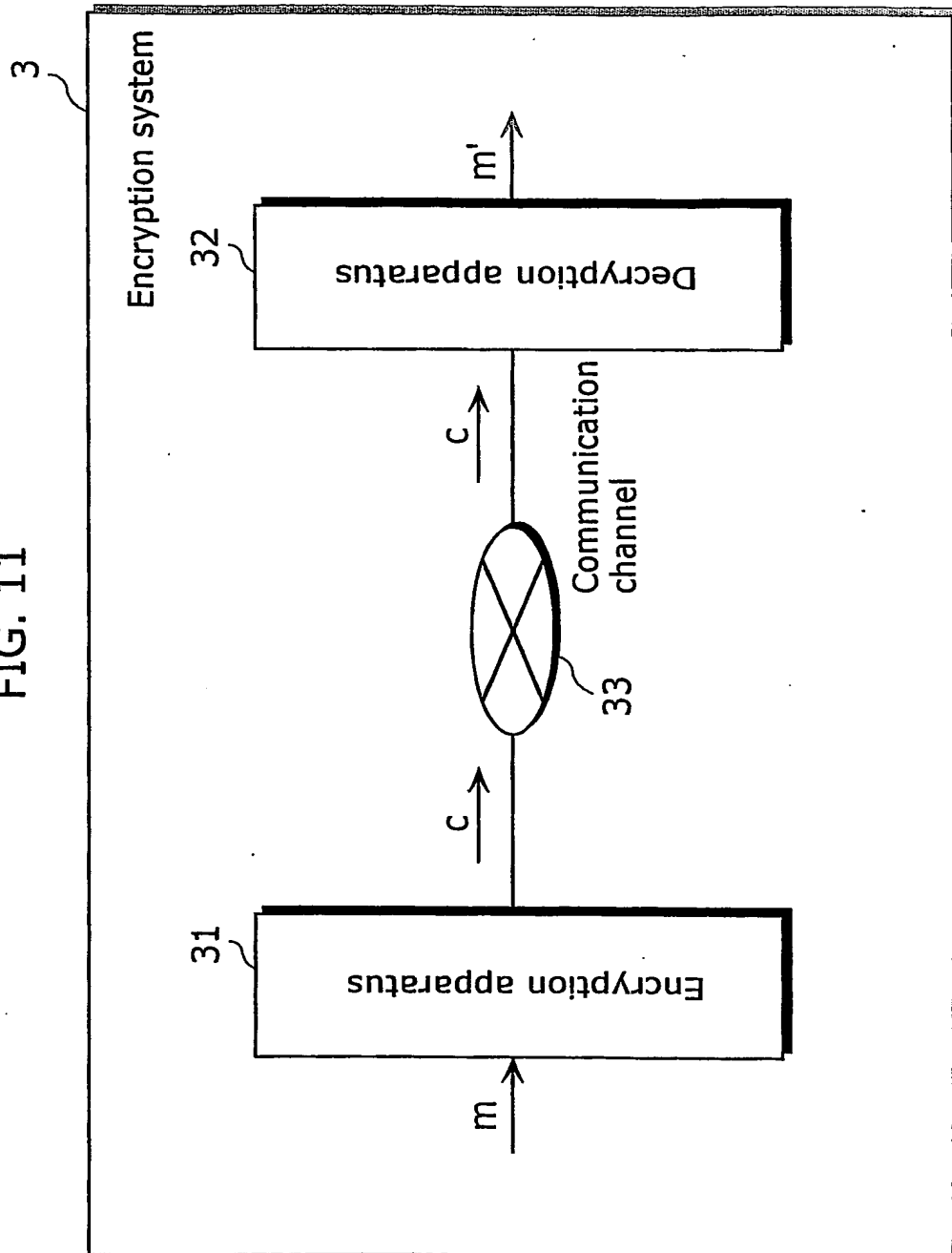


FIG. 12

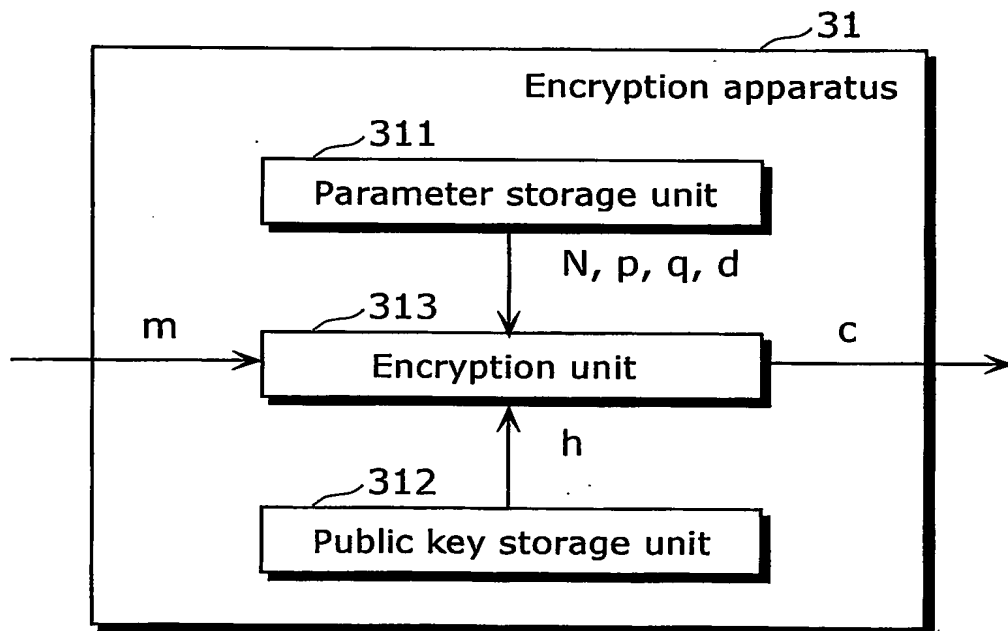


FIG. 13

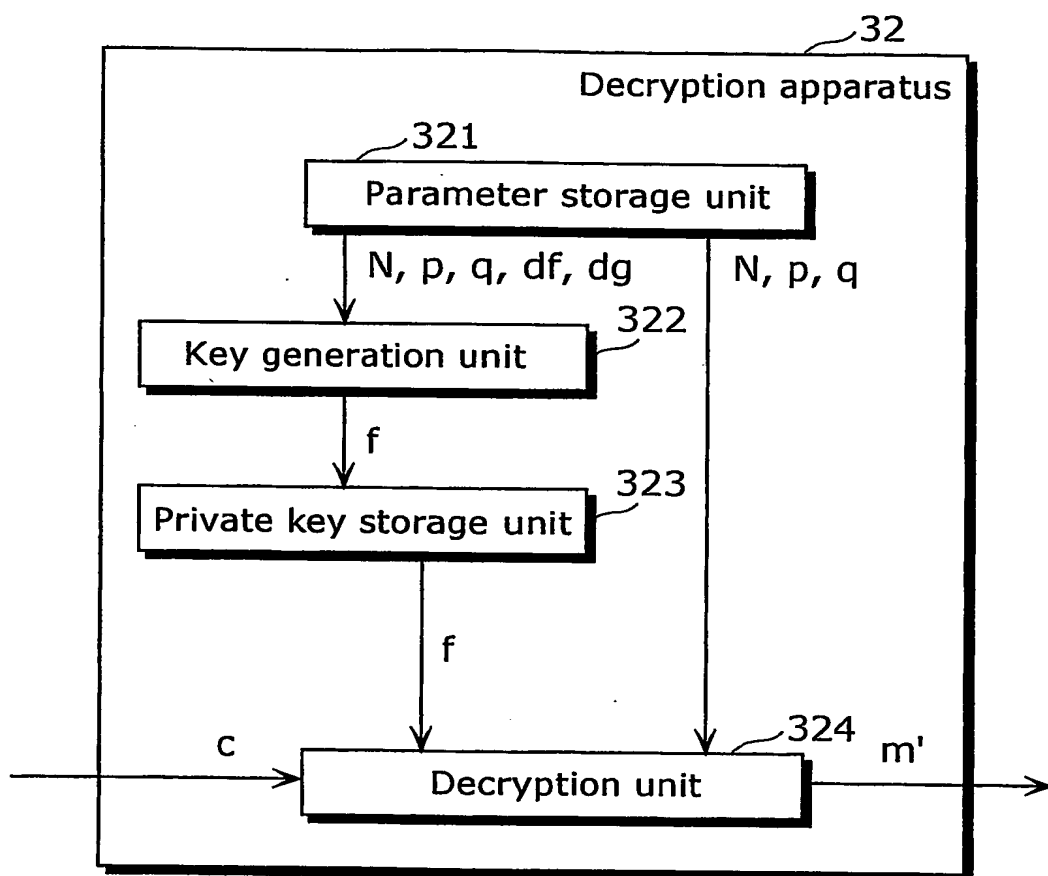


FIG. 14

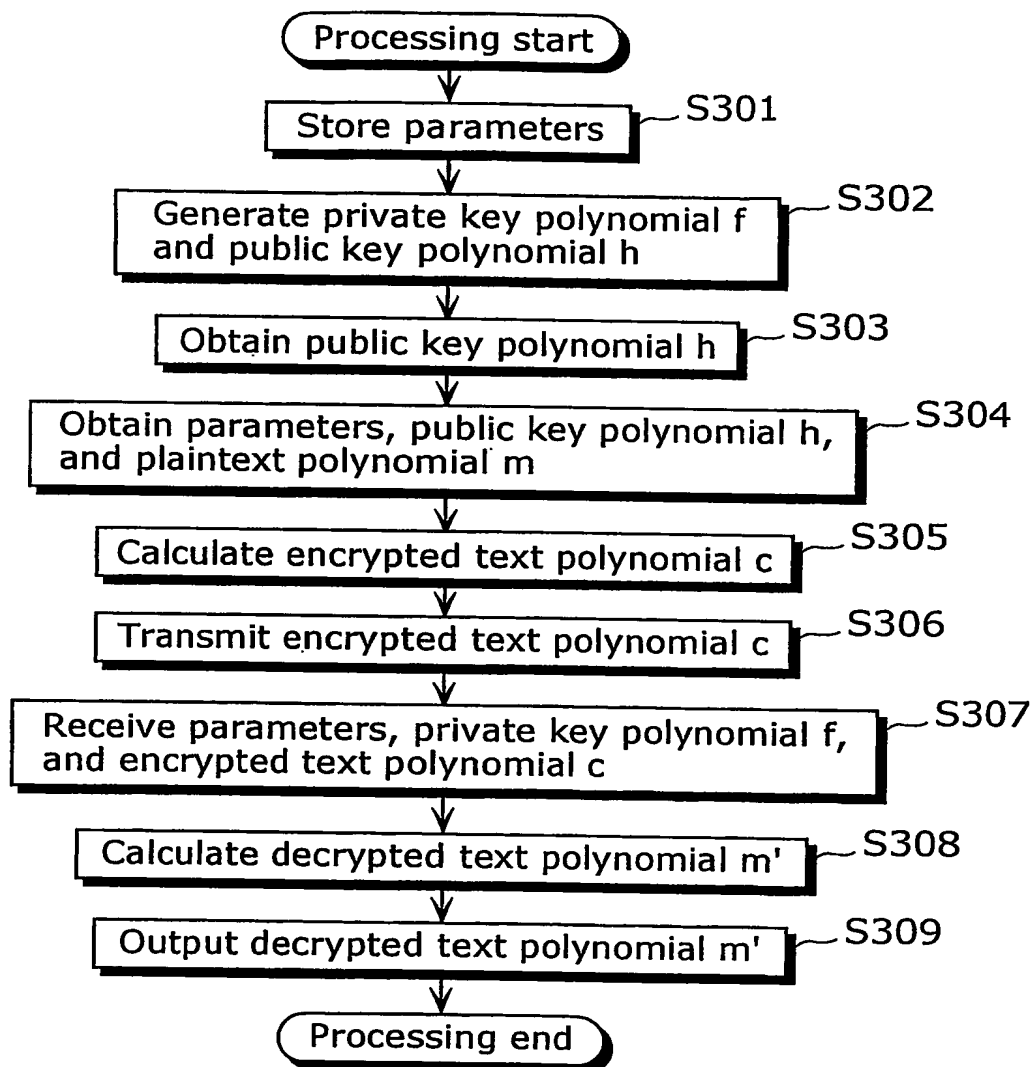


FIG. 15

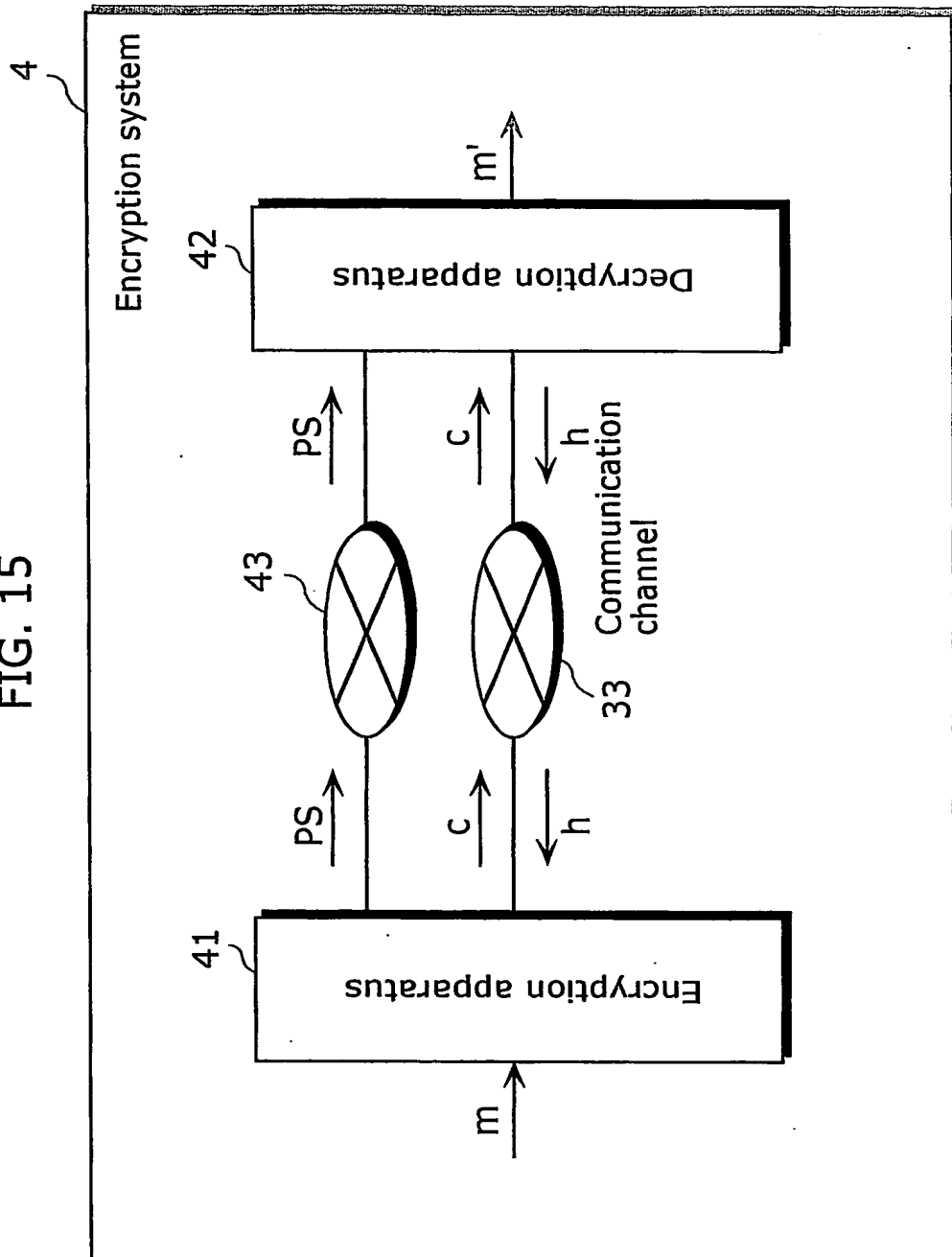


FIG. 16

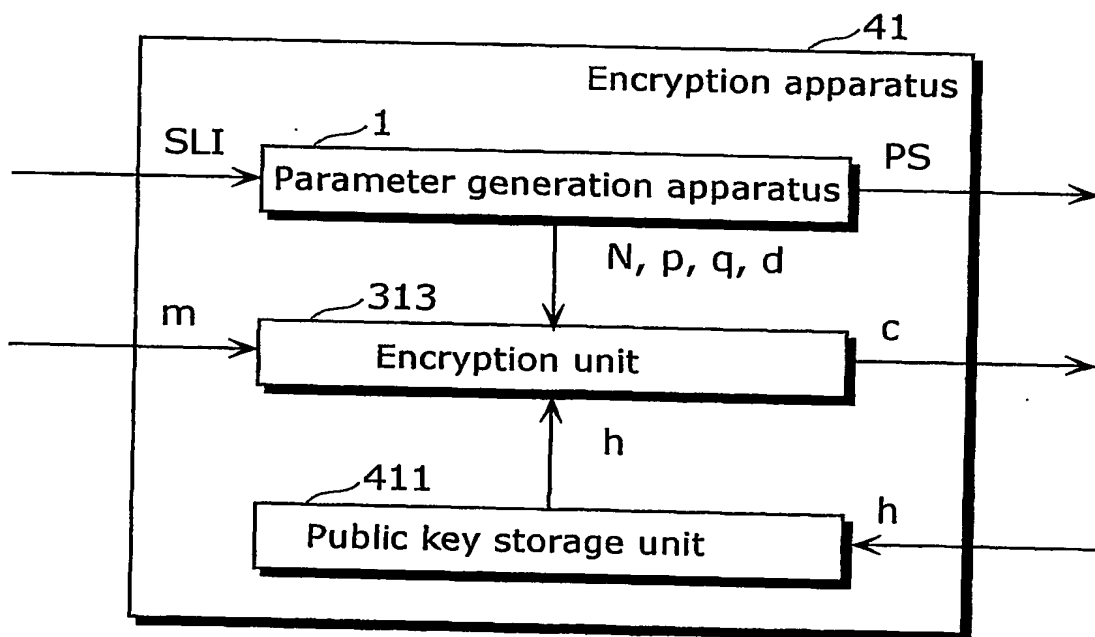


FIG. 17

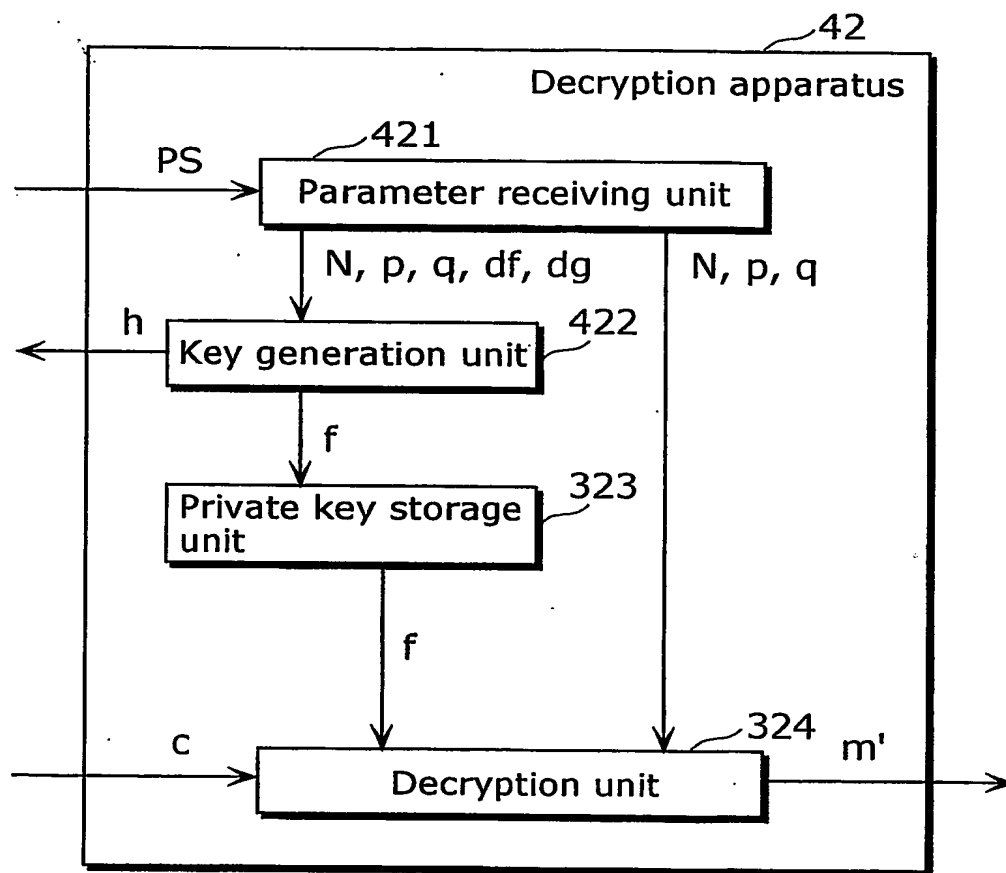


FIG. 18

